캡스톤디자인II

- 졸업작품 아이디어 제안서 -

UnderDog 임연주, 송영준, 곽수진

상명대학교 컴퓨터공학과

지도교수: 이종혁(jonghyouk@smu.ac.kr)

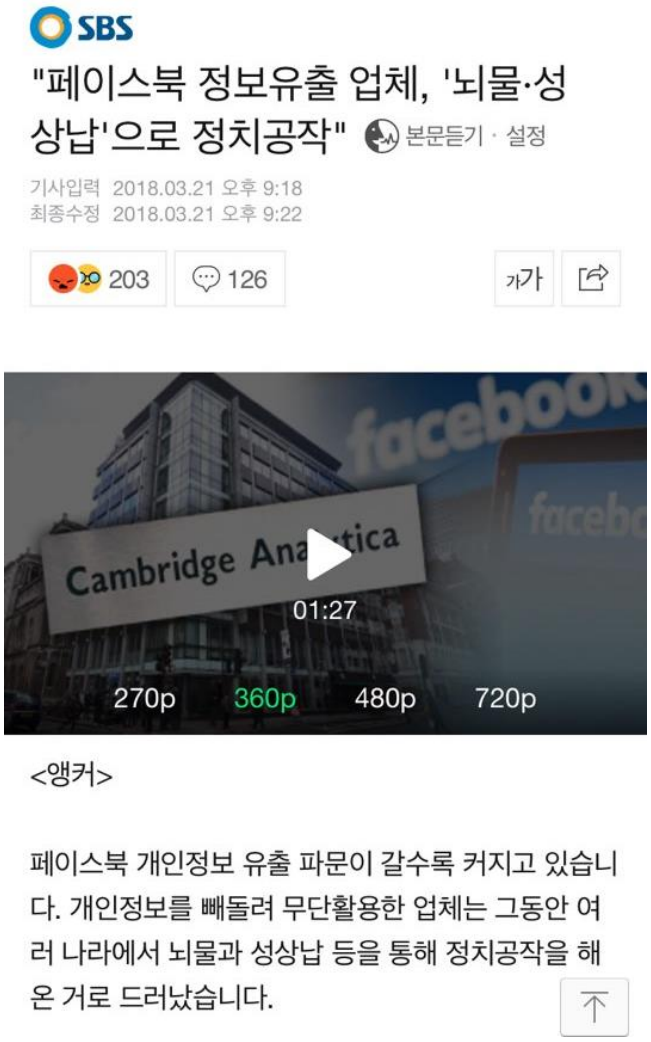
목 차

프로젝트 소개

- 개요
  - 블록체인 기술을 활용하여 디지털 ID를 관리하는 시스템 개발
    - Provider가 Partner에게 ID 및 인증 관리 인프라를 제공
    - 하나의 ID만 인증하면 원하는 다른 서비스들도 이용가능
      - e.g., 특정 통신사 ID가 있는 고객의 경우, 제휴처에서 간단한 숫자 입력시 이용가능
    - Microsoft, SK C&C 등에서 현재 도입 중

프로젝트 소개

- 개발 배경
  - 기존 클라우드 환경에서 데이터 유출 사고 급증
    - 안전한 개인정보 관리 필요성 대두



- 개발 목표
  - 제안된 논문을 기반으로 시스템 구현
    - “BIDaaS (Blockchain based ID as a Service)”, IEEE Access 2017.12

관련 연구

- 블록체인 (Blockchain)
  - P2P 네트워크 환경에서 거래 데이터를 블록에 저장하고 이 블록들이 연결되어 체인을 이루는 기술
    - 2009 년 1 월, 사토시 나카모토 (Satoshi Nakamoto)에 “비트코인”에서 처음 제안됨
  - 특징
    - 중앙 관리자가 필요하지 않음
    - 분산형 원장 구조로 위,변조가 어려움
  - 현재 금융, 에너지, 물류 등 다양한 분야에서 활용

관련 연구

- IDaaS (Identity as a Service)
  - 클라우드 또는 SaaS(Software as a Service)를 통해 제공되는 ID 및 접근 관리 서비스
  - 사용자는 하나의 ID로 연관된 모든 애플리케이션, 소프트웨어 등에 로그인 가능
  - 새로운 서비스 이용시 인증, 권한, 데이터베이스 관리 등의 반복성을 피하기 위해 만들어짐

  - ID, PW 분실우려 감소
  - 비용과 시간의 절감

프로젝트 기능 분석

- 엔티티
  - Provider
    - Partner에게 BIDaaS 서비스 제공
    - 블록체인을 유지 및 관리
    - User의 가상 ID, 공개 키 등을 서명과 함께 블록체인에 기록함
  - Partner
    - User에게 서비스 제공
    - 블록체인에 읽기 권한만 부여됨
  - User
    - 애플리케이션, 웹 사이트 등을 사용하는 일반 사용자

프로젝트 기능 분석

- 요구사항 분석 (1/3)

구분	기능	엔티티	내용	비고
사용자 정보 생성	개인키, 공개키 생성	User	User 자신의 개인키와, 공개키 생성	OpenSSL (RSA)
	Virtual ID 생성	User	User 자신의 공개키를 통해 Virtural ID 생성	OpenSSL(SHA 256 or Keccak-256)
	User 정보 전송	User, Provider	User의 공개키와 Virtual ID 암호화, 복호화	OpenSSL (AES)
블록체인 등록	Provider 디지털 서명	Provider	Provider의 개인키로 전송 받은 정보를 디지털 서명	OpenSSL (ECDSA)
	사용자 정보를 블록체인에 저장	Provider (풀노드)	공개키, Virtual ID, 디지털 서명 정보를 트랜잭션 input에 삽입	eth.sendTransaction ({input: })

프로젝트 기능 분석

- 요구사항 분석 (2/3)

구분	기능	엔티티	내용	비고
상호 인증	디지털 서명	User	Virtual ID, Nonce를 자신의 개인키로 디지털 서명	OpenSSL (ECDSA)
	서비스 접근 요청 메세지 전송	User, Partner	User가 Partner에게 서비스 접근 요청(Virtual ID, Nonce, 디지털 서명)	HTTP Post
	사용자 정보 등록 여부 확인	Partner (풀노드)	블록체인에 User Virtual ID 확인	eth.getTransaction(), eth.getTransactionReceipt()
	공개키 획득	Partner (풀노드)	블록체인에 저장되있는 User 공개키 획득	eth.getTransactionReceipt()
	공개키 비획득	Partner (풀노드)	블록체인에 User 정보가 없음을 사용자에게 알림	HTTP Post
	디지털 서명	Partner	획득한 User의 공개키를 통해 수신한 메시지의 디지털 서명 검증	OpenSSL (ECDSA)

프로그램 기능 분석

- 요구사항 분석 (3/3)

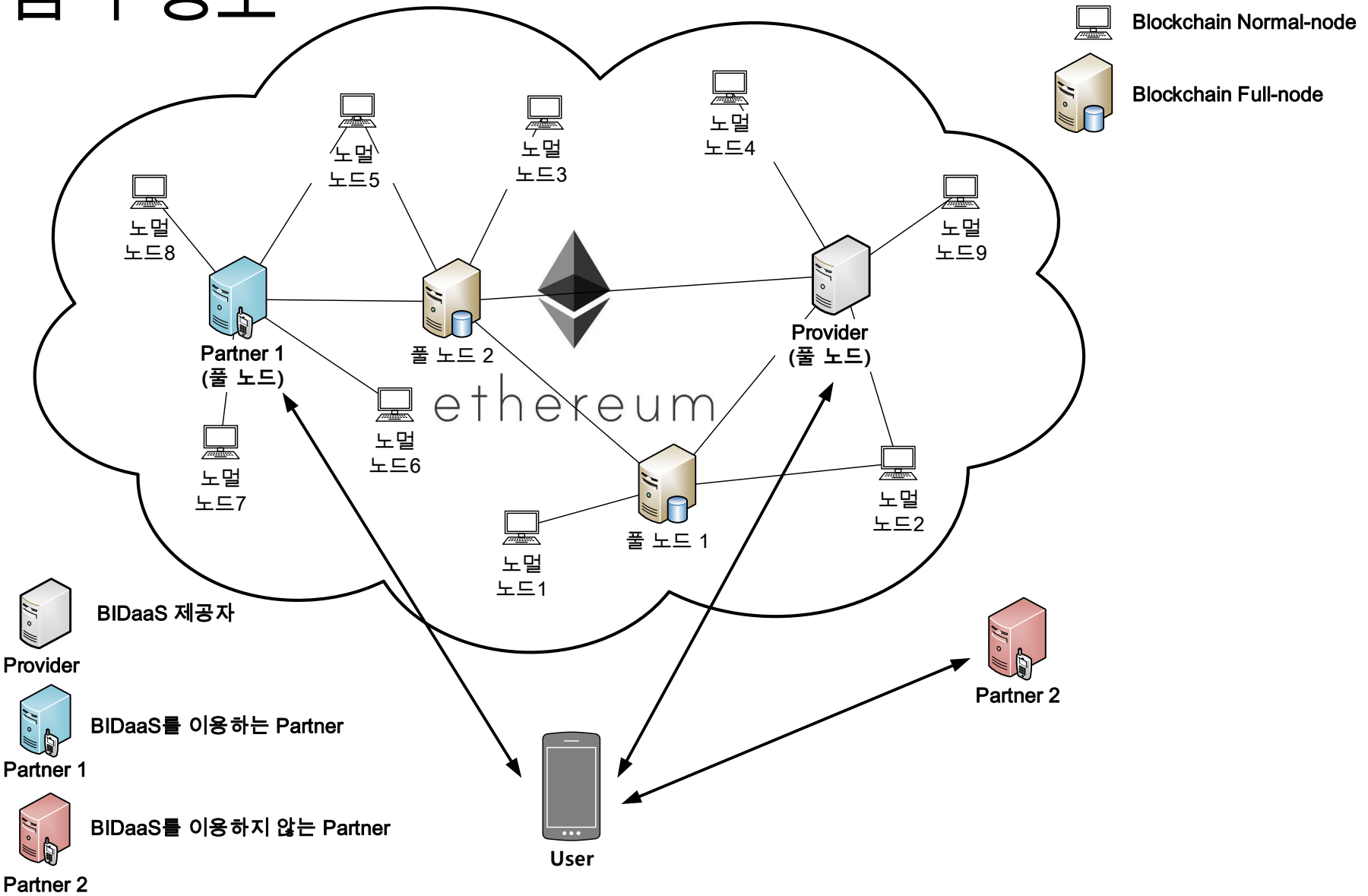
구분	기능	엔티티	내용	비고
상호 인증	Partner 공개키 전송을 위한 메시지 암호화	Partner	획득한 User의 공개키로 메시지(Virtual ID, Nonce+1, Partner의 공개키) 암호화	OpenSSL (RSA)
	메시지 전송	Partner, User	메시지(Virtual ID, Nonce+1, User의 공개키로 암호화한 데이터) 전송	HTTP Post
	메시지 복호화/검증, Partner 공개키 획득	User	User의 개인키로 암호화된 메시지 복호화, 응답 메세지 Nonce+1 검증, Partner 공개키 획득	OpenSSL (RSA)
	Partner의 공개키로 암호화	User	획득한 Partner의 공개키로 메시지 (Virtual ID, Nonce+2) 암호화	OpenSSL (RSA)
	메시지 전송	User, Partner	메시지(Virtual ID, Nonce+2, 암호화된 데이터) 전송	HTTP Post
	암호화 메시지 복호화/검증	Partner	Partner는 자신의 개인키를 이용해서 암호화된 메시지 복호화	OpenSSL (RSA)
	BIDaaS 서비스 로그인	Partner, User	Virtual ID를 기반으로 로그인 완료	HTTP Post

구현

- 개발환경 구성
  - Provider
    - 이더리움 블록체인
      - Go-ethereum: 1.8.2-stable
  - Partner 서버
    - Apache: 2.4 (Ubuntu)
    - PHP: 7.0
  - User(모바일 유저)
    - 운영체제: 안드로이드 롤리팝(5.0)

구현

- 시스템 구성도


Blockchain Normal-node
Blockchain Full-node
노멀 노드5
노멀 노드3
노멀 노드4
노멀 노드8
노멀 노드9
Partner 1 (풀 노드)
풀 노드 2
Provider (풀 노드)
ethereum
노멀 노드6
노멀 노드7
노멀 노드2
풀 노드 1
노멀 노드1
BIDaaS 제공자
Provider
BIDaaS를 이용하는 Partner
Partner 1
BIDaaS를 이용하지 않는 Partner
Partner 2
User
Partner 2

구현

- 프로젝트 참여도
  - 팀원 역할

	임연주	송영준	곽수진
블록체인 분석	2017년 후반기 진행		
IDaaS 환경 정의		O	O
엔티티 및 기능 명세	O	O	O
인증 프로세스 정의 및 명세	O	O	O
블록체인 네트워크 구현 및 연동	O	O	O
모바일 User 구현		O	
웹 인터페이스 구현			O
테스트	O	O	O
보완 및 검증	O	O	O

구현

- 프로젝트 진행 계획
  - 간드 차트

3월 2일 ~ 5월 8일	Week								
	1	2	3	4	5	6	7	8	9
IDaaS 환경 정의	■	■							
엔티티 및 기능 명세	■	■	■						
인증 프로세스 정의			■	■	■				
블록체인 네트워크 구현 및 연동				■	■				
웹 인터페이스 구현						■	■		
테스트							■	■	■
보완 및 검증							■	■	■

감사합니다!